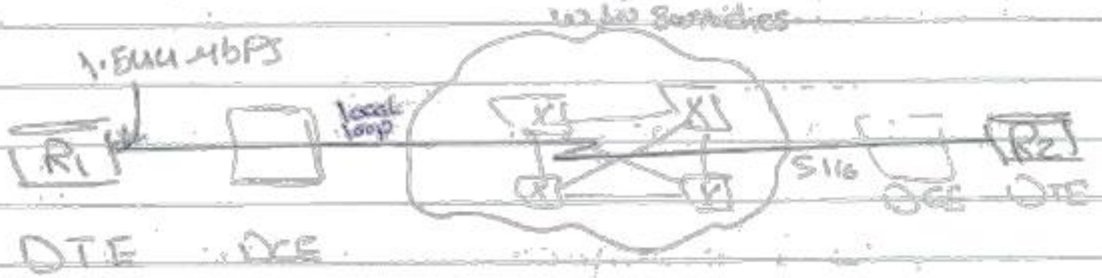
2018

WAN Technology papers

Written by:
Eng.
Amgad M. Mesallam
Edited by:
Eng. Abeer Hosni

WAN introduction



DTE . DCE

Data → Data Communication equipment

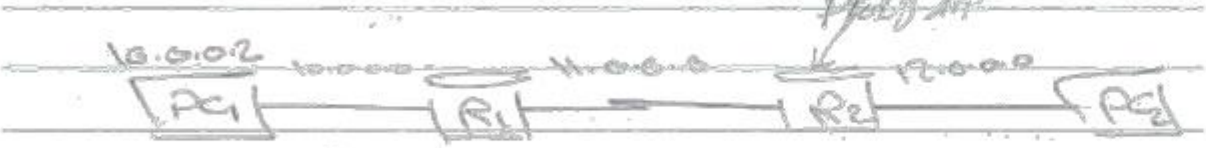
Terminal equipment

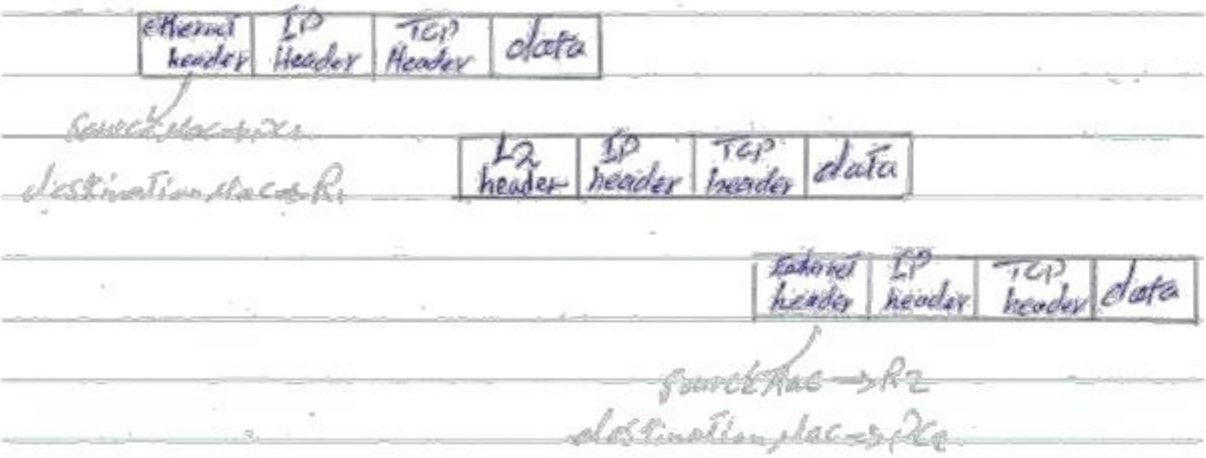
DCE → analog → Modem → digital (CSU/DSU)	Communication Co. Carrier Co. Teleco

Local loop: السلكة اللي بيربطني كـ Coustmer بالسنترال

Demarcation point:
a physical point that defines the responsabilities of the Coustmer and the responsabilities of the ISP
هي نقطة Physical في الفصل بين ال ISP والسنترال بتميزلي ايه هي مسئولية ال Coustmer ومسئوليات ال ISP
وهي ال Splitter في حالة ال DSL.

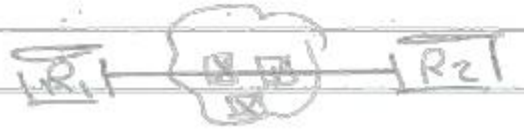
CPE: Coustmer premisous equipment





(wan technologies)

* Dedicated Circuit Switching (leased line)



The data always travel from Source to destination using the Same Path
وبالتالي حجز ليا انا لوحدي ومحدش حيشاركني في الـBandwidth

ميزته انه بـ security ماشي عليه بس غالي

Terminal
→ American   → Europe   → Japan

T_1, T_2, T_3, E_1, E_2, E_3, J_1, J_2, J_3, STM

1.544 Mbps   2Mbps E ⇒ 32 channels

1544 ⇒ 24×64 + 8

STM ⇒ 155 Mbps

اللي بنشتغل بيه ال ISP

* on-demand Circuit Switching:-

It is a leased line for a short period of time

exg: dial-up

لما باطلب الخط بيبقى بتاعي بس لفترة معينة.

• ISdn

بيقسم الساعة لـ 2 channels واحدة بتنقل عليها Data وواحدة بتنقل عليها Voice

Voice 64KbPS

Data

ولم تستمر تكنولوجيا الـ ISDN طويلاً نظراً لظهور الـ DSL.

- Packet Switching:

الفرق بين ال Circuit Switching وال Packet Switching

في ال Circuit sw. لازم ال Connectivity بين ال Source
وال destination لازم تكون Established وال data دائماً
بتاخد نفس المسار بين ال source وال destination

Packet switching

ال Data مش بتمشي في نفس المسار بين ال source وال destination
وبتتجمع في ال Destination

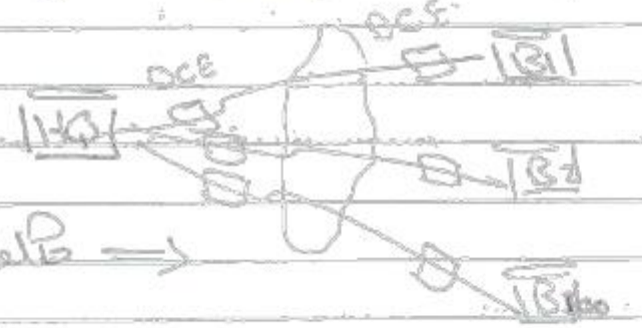
MPLS:

A WAN technology serves as the underlying network to carry multiple types of network traffic such as IP, ATM, Ethernet, and DSL

* Packet switching — ٢ انواع من الـ

- X.25
  (reliable - error correction) مش شغالة
  والمشكلة كانت الجودة بتاعتها قليلة

- Frame relay — الفكرة لقناة ١م٢م٣م٤م



مكلف جداً ⟵

الحل ⇐ Frame Relay

(سرعتها عالية T3)

وصل الـ serial port
والسرعة عالية
علشان الـ HQ
ومش محتاج leased line
والـ FRSW بيشتغل DCE

مشاكله ⇐ ① Shared Bandwidth
② low security.

CIR ⇒ اتفاقية بين الـ customer وبين الـ ISP
وبيوصل Minimum Bandwidth وممكن يزيد في وقت غير الذروة
(Committed info rate)

Frame relay ⇒ packet (1500 Byte) MTU

---

* في الـ FR الـ MTU تبقى على هيئة Packets بينما في الـ ATM على هيئة Cells.
يتمشى في هيئة Cells ذو حجم ثابت " ATM.
(Cells = 53 byte = 48 byte data + 5 byte header)

لا يكون حجم الـ Cell قليلة كدة بيقلل الـ Congestion
في الشبكة وسرعتها وصلت لـ 40 Gbps
وبيستخدموها في الاتصالات ديتا وبين بعض

- Broadband techologys-

- DSL (Digital subscriper line)
- Satellite
- Cable TV (DOCSIS)

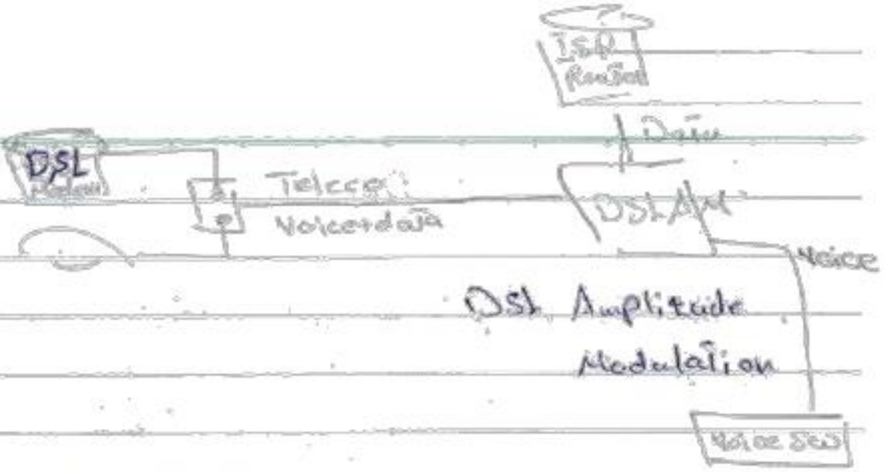
DSL

↳ ADSL (asymmetric DSL) — غير متساوي

↳ SDSL (symmetric DSL) — متساوي

ADSL ⇒ سرعة الـ Download أسرع من الـ upload
بنسبة 5 : 1

SDSL ⇒ سرعة الـ Download تساوي سرعة الـ upload
بنسبة 2 : 2 مش بيشغل التليفون.
1 : 1



PPP Protocol

Point to Point Protocol

بيعملي encapsulation في L2

دخل لـ PPP الان

- Standard HDLC

" High level Data link Control)

Flag	Address	Control	data	FCS	Flag

مبيعرفش انه بيشغل Protocol واحد بس

- Cisco HDLC

Flag	Address	Control	Protocol type	data	FCS	Flag

بيشغل اكتر Protocol بس مشكلته انه Cisco علشان

كدة ظهر الـ PPP

L2 — WAN

L2		WAN
LLC (Logical Link Control)	≡	LCP (link Control Protocol)
MAC (Media Access Control)		NCP (Network Control Protocol)

Ncp, LLC => بيتفاوضوا مع ال network layer علشان يستوعبوا
هيشتغلوا بأي نوع من ال Addressing

Lcp => علشان ال R يـ connect على ال R التاني
لازم تتوافق ال properties بتاعتهم وبعد كده ال NCP هي اللي
بيظبط الكلام ده.

PPP properties:

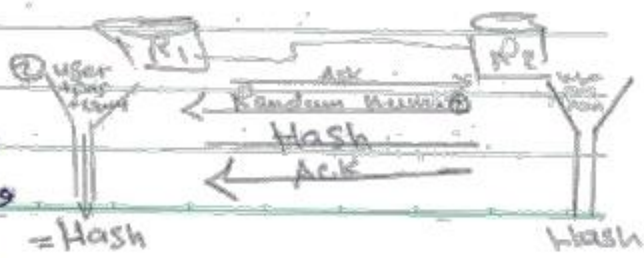
- authintication

بأظبط username و password على الراوترين Two Routers ←
بـ connect على بعض

- ↳ PAP
  - → 2way handshake
  - → 2way authentication

- ↳ CHAP => 3way hand shake.

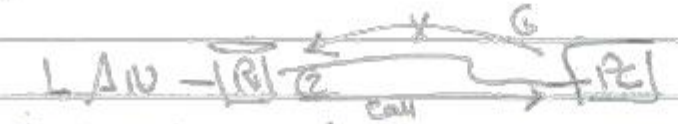
- R1 بيريد الدخول على R2 فيقوم
R2 بإرسال random nu لـ R1
ويقوم R1 بعمل hash من username
والباسورد وال random nu وإرسال
ال hash للطرف الآخر



والطرف الآخر يقوم بنفس العملية فإذا أسفرت عن نفس نتيجة الـ hash قام بعد ذلك أن الـ username والـ pw صحيحة ويقوم بإرسال الـ Success Ack.

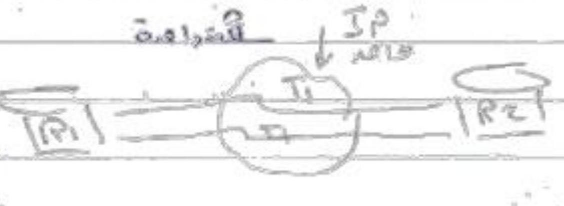
- Call back :-

يقوم الراوتر بفصل الـ connection الذي بدأه الـ user ويقوم بعمل الـ connection بنفسه لتقليل التكلفة.



- Multi link :-

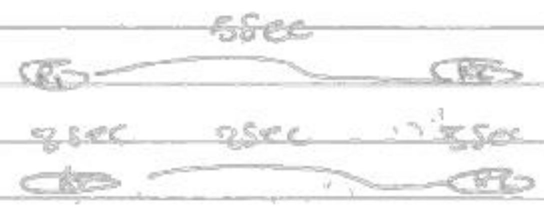
التعامل مع أكثر من link كأنهم int واحد وإعطاؤهم IP واحد لزيادة الـ BW.



Compression :-

↳ predictor
↳ Stack
↳ MPPC

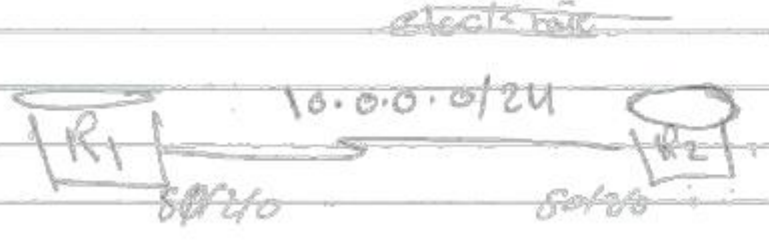
→ Microsoft point-to-point Compression



أقوى في الـ Compression

يفضل الـ load هيزيد

Lab



R1# show controllers

R1# config t

R1(config)# int s0/2/0

R1(config-if)# encapsulation ?

R2(Config-if)#encapsulation ppp ↵
R2#show Ip int b ↵

=

authintication

[R1] —————— [R2]

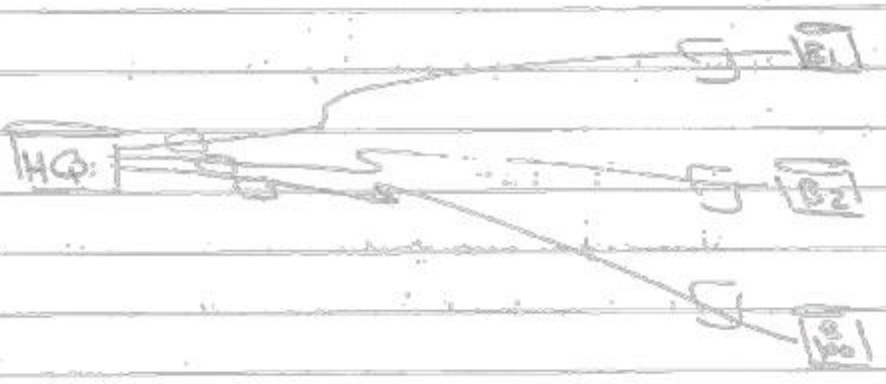
username: R2 username: R1
pass: CCNA Pass: CCNA

R1(Config)#username R2 pass CCNA
R2(Config)#username R1 pass CCNA

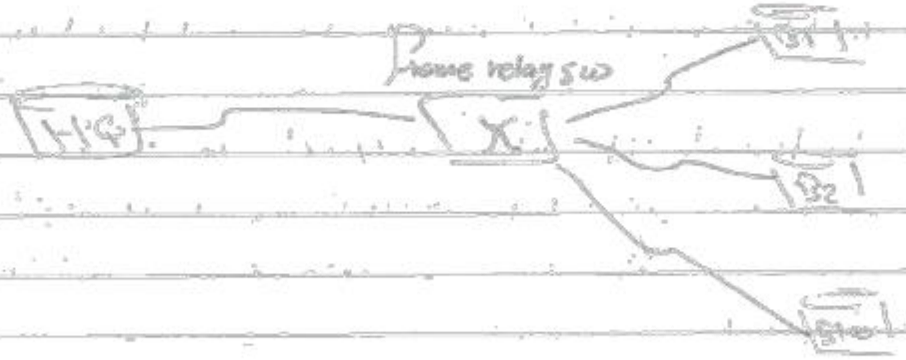
R1(Config) int S0/2/0 ↵
ppp authentication ?
ppp authentication CHAP
(LCP open)

R1# show ip int br
اذا كانت حالة ال int هي up/down فإن ذلك بسبب:
1. encapsulation mismatch
2. authentication failure
وفي تلك الحالة سيكون حالة البروتوكول LCP هي closed
وليس open كما يظهر من أمر R1#show int S0/2/0
* ملحوظة)
الراوترات الحديثة تكون قيمة ال clocking configured by default. ولتغيير قيمة ال clock rate:
R1(Config-if)# clock rate [ ] ← S0/2/0
↑ DCE router

«Frame relay»



الحل



مشكلته ⇐ ① الـ (Securiy)

علشان الـ Bw ⇐ shared

علشان الـ Frame Relay sw مخزن بتوع عليه كذا شركة

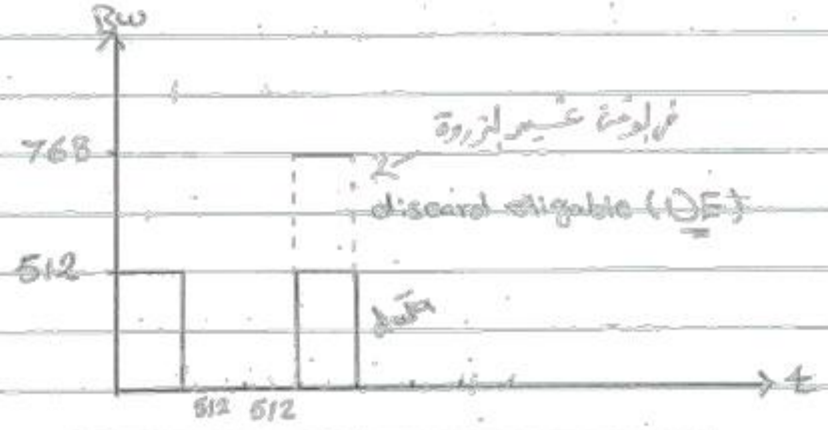
والـ ISP عمل الحاجة اسمها CIR

Committed information rate

معناها ان الـ ISP هيضمنلي min. Bw

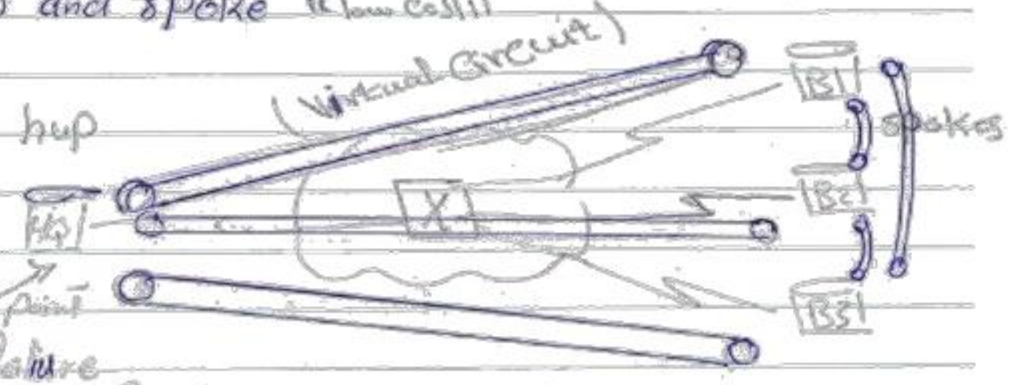
مش هاقل عنه في وقت الذروة مثلاً (512)

تشبه [illegible] Frame Relay Technology



Frame Relay topologies:-

① hup and spoke "low cost"



Single point of failure

↳ يعني لو وقع الشبكة
كلها هتقع.

② Partial Mesh

هاوصل ماسورة بين B1 و B2

* توصيل بعض الـ VCs بين الـ branches اللي عندها داتا مهمة

③ Full Mesh

هاوصل ماسورة بين كل الـ B و الـ HQ وكذلك بين الـ branches وبعض

يعني [illegible] Data [illegible] الـ source [illegible] Destination Direct

في حالة الـ Full mesh لو عاوز أعرف عدد كام
Virtual Circuit عن طريق المعادلة

$$VC = n(n-1)/2 \quad (n = \text{No. of R})$$

Virtual Circuit

- PVC الشائع
  - Permanent VC
  - دايماً مستمرة متصلة وعادية
- SVC
  - Switched VC
  - قبل ما أقدر أبعت الداتا
  - لازم الـ circuit تبقى
  - established

في تقنية الـ Frame Relay مفيش حاجة اسمها MAC
لأن هي متوصلة بـ Serial int.
والبديل عنها هو DLCI
Data Link Connection Identifier
وهو ده الـ L2 addressing.

وكل VC بعملها Create لازم على كل طرف منها يكون
عليها DLCI الـ Source DLCI, Destination DLCI
وده الـ Configuration انا بعملها.

DLCI => Locally Significant per Segment.
رقم الـ DLCI لازم يبقى unique على الـ Routers

DLCI

Static
يعني بـ Execute بإيدي
"manually created by Configuration."

inverse Arp
يعني بـ R بياخد DLCI من الـ FRSW الموجودة.
"بيعمل الـ DLCI بطريقة Dynamic"

ولو لقيناه شغاله تمام بتعرض الاتي جوه الـ Int Active

LMI Protocol:
"Local Management Interface"

عبارة عن Signal مابين الـ Source والـ Destination
بيقولوا فيه حالة الـ Int

1. Active — يعني الطرفين مفيش مشكلة
2. In Active — يعني الطرف التاني فيه مشكلة
3. Deleted (DLCI is deleted on my side) — يعني المشكلة عندنا احنا وغالباً بتبقى الـ DLCI

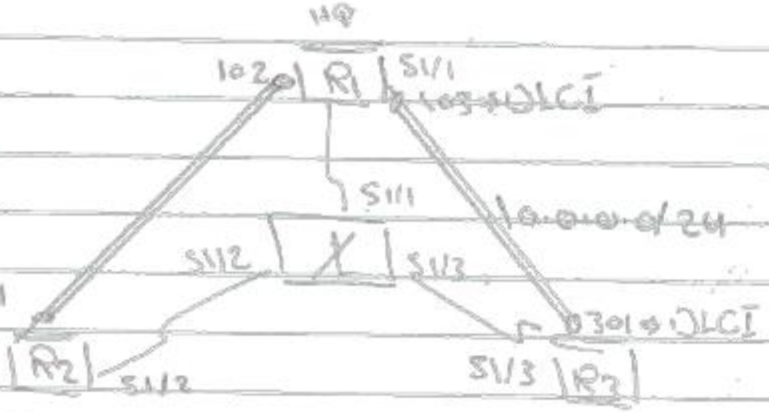
LMI Types:-

- Cisco (default)
- ANSI
- Q.933a

(Locally significant per segment)

لو حصل mismatch لنوع ال LMI بين طرفين ، والاتنين
مش هيحصل لـ int تغيير up/down.

"Frame relay Configuration"



hub and spoke

GNS ⇒ R C3700

R0 ⇒ hostname FRSW

line Console 0 ↵

→ first, Configuring router Cisco as a frame relay switch.

```
FRSW # Config t ↵
FRSW(Config)# frame-relay switching ↵
FRSW(Config)# int S1/1 ↵
(Config-if)# No ip address ↵
(Config-if)# encapsulation frame-relay
(Config-if)# Frame-relay ?
(Config-if)# frame-relay intf-type dce
(Config-if)# clock rate 64000 ↵
(Config-if)# No frame-relay inverse-arp ↵
PVC { # Frame-relay route 102 int S1/2 201 ↵
      # frame-relay route 103 interface S1/3 301 ↵
# No shut down ↵
# end
```

(side notes: encapsulation … * / dce … * / Recommended … * / static … / DLCI … / DLCI …)

* show run int s1/1 ↵ بيجيب Running Config بتاع إنت

باخد Data ⇐ copy و paste

في ملف TXT وبعدله

frame-relay route 201 interface s1/1 102

* int s1/2
* paste ↵

* int s1/3
* paste ⇒ frame-relay route 301 int s1/3 103 ↵

* show frame-relay route ↵

---

r1(config)# int s1/1 ↵

r1(config-if)# ip add 10.0.0.1 255.255.255.0 ↵

* encapsulation frame-relay ↵
* No frame-relay inverse-arp
* frame-relay map ip 10.0.02 102 broadcast ↵
* frame-relay map ip 10.0.03 103 broadcast ↵
* No shut ↵

```
r2(Config)# S1/2
r2(Config-if)# ip add 10.0.0.2 255.255.255.0 ↵
    # encapsulation frame-relay ↵
    # No frame-relay inverse-arp ↵
    # frame-relay map ip 10.0.0.1 201
    # frame-relay map ip 10.0.0.3 201
    # No shut ↵
```

```
r3(Config)# S1/2 ↵
    # ip add 10.0.0.3 255.255.255.0 ↵
    # encapsulation frame-relay ↵
    # no frame-relay inverse-arp ↵
    # frame-relay map ip 10.0.0.1 301
    # frame-relay map ip 10.0.0.2 301
    # no shut ↵
```

```
r1 # show frame-relay map ↵
r2 # Trace route 10.0.0.3 ↵
```

هلاقي انه بيعدي على R1 الأول بعدين R3

علشان انا عامل الـ R مش بيعدي الـ Broadcast :- Broadcast

ولا الـ Multicast دي حاجة انا من شايفها ودا في R

خلي بالك هنا انه عاملة Routing protocol وهيحتاج اني ابعت الـ update ⇐ Broadcast او multicast

⇐ Recomended اني ابعت Broadcast في سيعر واحد بس لغاية.

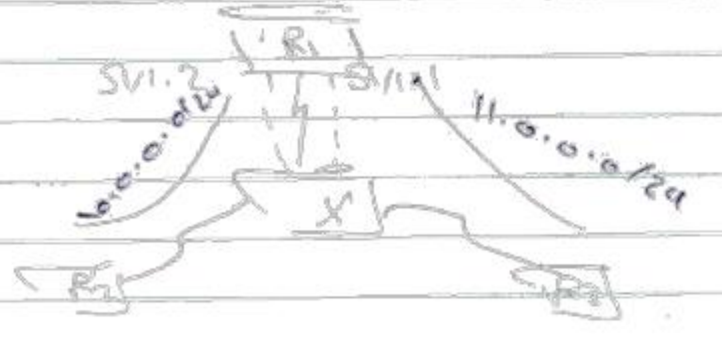
+ splite-Horizon issue

دا بالنسبة الـ update هيقابلها مشكلة في حاجة اسمها الـ Routing Protocol ⇐ EIGRP & RIP اسمه الـ split Horizon هيمنع انه الـ update يرجع على نفس الـ ... اللي جاله.

- No ip split-Horizon eigrp 1 ده بس كده انا بقيت عرضة الـ Routing Loop

- full mesh اني استعمل بس كده محتاج cost عالي ومش منطقي

*** - sub interfaces
(point-to-point sub interfaces)



r1 # int S1/1.1 ?
int S1/1.1 Point-to-point ↵
Frame-relay interface-Dlci 102 ↵
وعطيه ip لـ R

(H.W)

لو حبيت اغير الـ LMI

r(Config)# int S1/1 ↵
r(Config-if)# Frame-relay LMI-ty ?

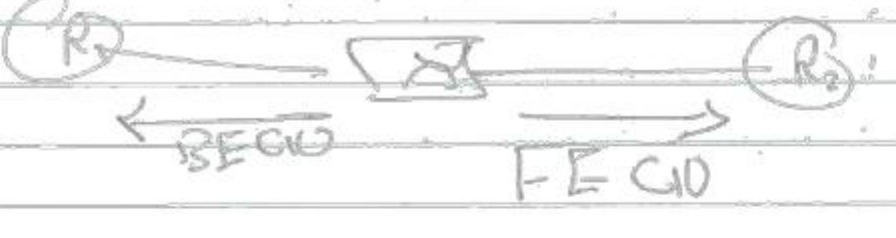
Frame Relay Congestion management

لو صار عندي Congestion

- Backward Explicit Congestion Notification
« BECN »

- Forward Explicit Congestion Notification
« FECN »

- Discard Eligibility



Network attacks

To understanding Network Security

٢ انواع الـ Network attack

① Physical Network attack

Physical installations:-

Mitigation → Secure equipment physically in a separate room
→ using Video Monitoring or wireless webcam.

② Reconnaissance attacks:-

ويقوم فيه باستطلاع لجمع المعلومات عن الشبكة قبل البدء بالهجوم الفعلي

a) packet sniffers
b) ping sweep
c) port scan
d) using internet database
e) google hack

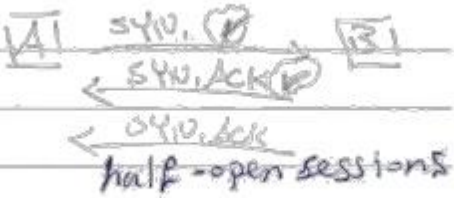
③ Access Attack

a) Password attack (brute-force & dictionary attack)
b) trust expolitation
c) man-in-the-middle

Dos attacks.

1. Ping flood.
2. mail Pomb — بعت بايعت E.mails كتيرة جداً لـ Destination معين والهدف منها إني أوقع الـ Destination
3. SYN flood

الـ Source بيبعت للـ Destination رسالة الـ TCP ← SYN بس



4. IP spoofing ← خداع

Distributed Dos :- D-Dos

هستخدم الـ PCs وأنا أعملهم هجمات ويعملوا attack على الـ Server

R1(config)# security passwords min-length 10

علشان أعمل الـ length بتاع الـ Password

" Auto secure "

CDP => Cisco Discovery protocol
Enabled by default

Finger => بيعرفني مين كل الناس اللي موجودين على الـ system بتاعي
Enabled by default.

الـ auto secure هي عبارة عن Configuration هيقفل كل الـ un-wanted services المفتوحة على الـ Router بتاعي

" Auto Secure "

Full

هيتفاعل معايا وهيسألني عاوز أفتح إيه وعاوز أقفل إيه

No interact

مش هيتفاعل معايا ومن وجهة نظر Cisco هيقفل اللي يقفله ويفتح اللي يفتحه من وجهة نظره هو.

Labs GNS:-

Enable mode

Router# auto secure ?

Router# auto secure ↵ ⇐ Full #

=

Router# auto secure no-interactive

* في حالة الـ full سيكون interactive من وسيسألك العديد من الأسئلة مثل عمل الـ enable للـ SSH أم لا و في حالة الإجابة بنعم سيقوم بعمل RSA key قيمته 1024، كذلك سيضبط min length للباسوردات قيمته 6 character، وهكذا.

Router # show run

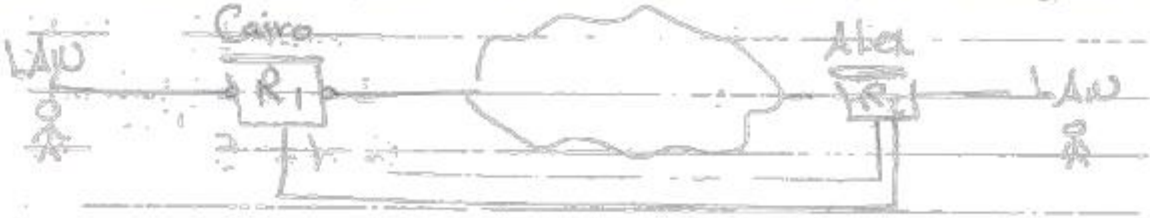
ستجد العديد من الـ services التي تم غلقها وإذا أردنا فتح service معينة لابد أن نعرف الأمر الذي يعمل لها enable

```
ex) R(Config) # ip http server
              # ip http secure-server
```

"VPN"

Virtual Private Network

- لعمل الـ traffic بين LAN و LAN أخرى عن طريق leased line أو VPN.



- معناه إن هيمشي الـ Data جوه Tunnel بس Private
الـ Private

- الـ Data بيتعملها Encapsulation بطريقة إن محدش يقدر [illegible]
خارجي.

VPN مميزات

Telnet => clear text
SSH => Encrypted
VPN => Tunneled.

1- Confidentiality :- => سرية الـ data
الحماية من اللي [illegible] عن طريق encryption
ومعنى [illegible] هو الـ Encryption

Symmetric | Asymmetric

Symmetric

هنا الـ key اللي بيشفر الـ data
هو نفس الـ key اللي هيفك التشفير
بعد data

R1 Key —— R2 Key

يعني هيبقى مشكلة في الـ Security في مرحلة تبادل
الـ Key في الأول.

Asymmetric

R1 —— R2
Public key —— Public key
Private key —— Private key
يشفر الـ data بالـ Public
ويفك التشفير بالـ Private

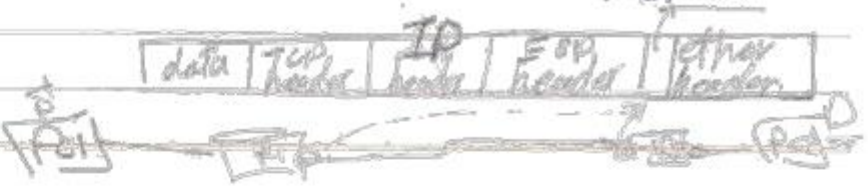
Symmetric	Asymmetric
* DES (56 bit) (112 bit active)	* RSA (SSH [illegible]
* 3DES (3*56=168 bit)	* Diffie-Hellman
* AES (128 bit) default	[illegible] vpn
(192 bit)	Group 1 (768 bit)
(256 bit)	Group 2 (1024 bit)
	Group 5 (1536 bit)

Asymmetric ⇐ هنشفر بال Key
symmetric ⇐ وهنشفر بال data

Negotiation protocols:-

2 protocols

AH	ESP
auth header	encapsulation Security payload
- بيعمل secure للdata فقط	- بيعمل secure للdata وال Ip header
- Security by auth.	- Security by auth
	- encryption.



- طريقة عمل ال Asymmetric :

يقوم ال destination بإرسال ال public key إلى ال source والذي يستخدمه في تشفير ال private key الخاص به والذي سيفك به التشفير ثم يقوم بإرسال ال encrypted private key إلى ال destination وبالتالي حتى ولو تم عمل sniff لل key فإنه يكون encrypted .
وإرسال ال source لل public key يكون داخل ال digital certificate .

2 authentication التحقق

pre-shared key

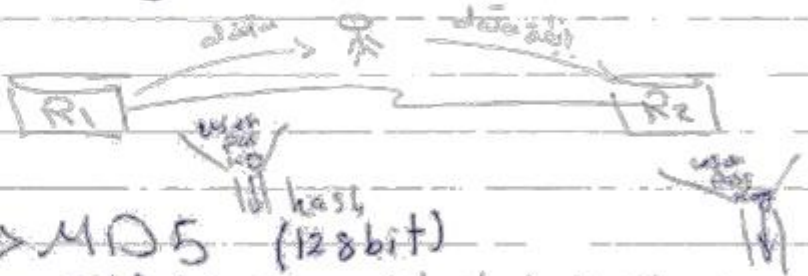
- يتم كتابته على الراوتر ويتم تبادله بعد تشفيره ولكن يفضل تغييره كل فترة كنوع من ال security .

PKI
public key infra

- في ال enterprise الكبيرة يصعب تغيير ال keys كل فترة ويفضل استخدام CA لإعطاء ال certificates وبا ال key .

✓(The data is not altered).

③ Integrity — معناها تأكد الـ data



2 Protocols → MD5 (128 bit)
→ SHA 1/2 secured hashed algorithm — hash اصدارات مع الـ keys تبدأ من 160

يقوم الـ source بإرسال الـ encrypted data مع hashed version لها

④ anti reply : يعني Random Key يتغير كل مرة.

* How to create a tunnel :-

- GRE (generic routing encapsulation)

ماهية بس بتشتغل إن يعمل auth. بس
ولا يوجد به encryption.

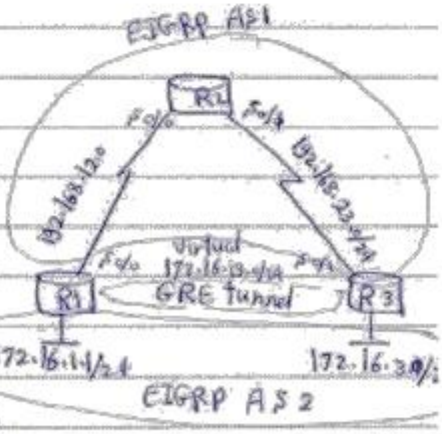
- PPTP (Point to Point tunneling Protocol)
نفس مشاكل الـ GRE وهي proprietary microsoft

- L2TP (layer 2 tunneling Protocol)
[L2F + PPTP]

- IP Sec : هو اللي create الـ tunnel
بتاعة الـ VPN

- لعمل الـ tunnel في cisco نستخدم الـ GRE أو الـ Ipsec

lab ② Configuring a basic GRE Tunnel.



① نشوف توزيع ال IP وال EIGRP.

- R1,R3 يمثلوا ال remote sites وال R2 بالنسبة لهم هو ال agency أو ساعد على اتصالهم بال VPN.

- GRE encapsulation is not encrypted by default, but can be encrypted through simple configuration techniques.

- R2 عنده لا يعني البيانات بين R1, R3 لا تنظر لل private networks وكل تنقل البيانات بناء على ال IP الخارجي والذي يعمل encapsulation لل private network.

- ال tunnel يشبه ال loopback في أنه logical (virtual) interface ولكنه يختلف عنه في أنه يستدعي وجود 2 routers لكي تكون ناحية بناء ال tunnel.

```
R1(config)# int tunnel 0
R1(config-if)# ip add 172.16.13.1 255.255.255.0
R1(config-if)# tunnel sorce s0/0
R1(config-if)# tunnel destination 192.168.23.3
R3(config)# int tunnel 0
R3(config-if)# ip address 172.16.13.3 255.255.255.0
R3(config-if)# tunnel source s0/0
R3(config-if)# tunnel destination 192.168.12.1
```

والآن النتيجة بين R1,R3 الفروض أن يكون successful

- الآن نقوم بتعريف ال routing protocol على R1, R3 بال eigrp رقم AS2.

```
R1(config-router)# network 172.16.0.0 , no auto-summary
R3(config-router)# network 172.16.0.0 , no auto-summary
```

} عرفت tunnel loopback

```
R1, R3 # show ip eigrp neighbors 2
```

حيث أن ال adjacency تم تكوينها على ال tunnel interface.

```
R1, R3 # show ip route
```

نجد أن كل راوتر يجد ال loopback int الخاص بالراوتر الآخر ولكن R2 لا يعرف عنهم شيئاً، وكل راوتر يجد الآخر متصلاً 172.16.13.0 الذي قمنا بإنشائه virtually.

Another situation:

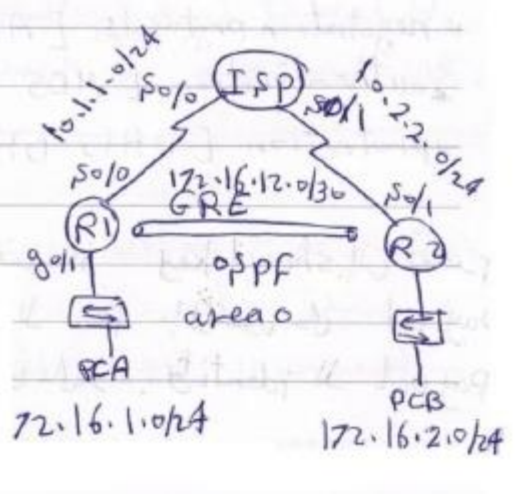
lab GRE (generic routing encap

- يتم استخدام ال GRE لنقل ال

ال IPV6 على IPV4 أو

لنقل ال multicast pkts لل OSPF و

ال EIGRP و ال streaming applications.



1) نقوم بعمل default static route على كل من R1 و R2 يرموا على ال ISP

R1 (config)# int tunnel 0

R1(config-if) # ip add 172.16.12.1 255.255.255.252

tunnel source S0/0

tunnel destination 10.2.2.2

وبالتالي R2.

R1,R2 # show ip int br

R1 # show int tunnel 0

tunnel source 10.1.1.1 , destination 10.2.2.2

tunnel protocol/transport GRE/IP

R1 # ping 172.16.12.2 successful

- نقوم بتعريف ال OSPF على ال tunnel وال LAN int.

R1 (config-router) # net 172.16.2.0 0.0.0.255 area 0

net 172.16.12.0 0.0.0.3 area 0

وكذلك على R2 وبالتالي ال LANs سترى بعضها بال OSPF بدون أن يكون ال ISP على دراية بتلك الشبكة.

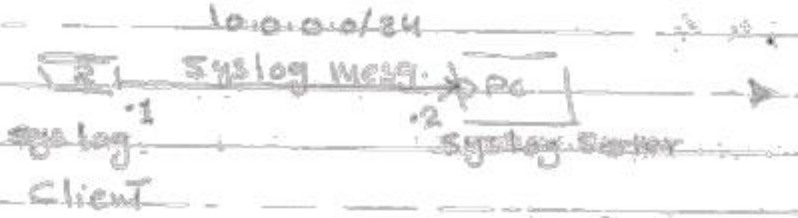
* سيناريو آخر)

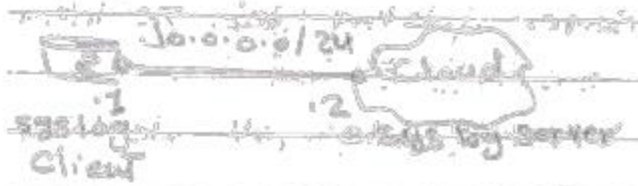
نقوم بعمل 2 processes من ال EIGRP احداهما تضم ال WAN links والأخرى تضم ال tunnel وال LANs. وفي تلك الحالة أيضا فإن ال ISP لن يكون على دراية بالشبكات ال LAN.

Syslog

عايز اعمل على Server علشان اخزن عليه بيانات واشوف ايه اللي حصل
عند ال R. او ال Sw.

GNS => Run as admin





Router# Config t
* int f0/0
* IP add 10.0.0.1 255.255.255.0
* no shut
* Ping 10.0.0.2 !!

(Setup Kiwi Syslog Server) Kiwi Syslog servr

Router (Config) # Logging on => يعمل Enable لل Log
enabled by default

(Config)# logging ?

logging 10.0.0.2 ↵

end

هلق بـ log الـ PA عم بيطلعلي هون

Time stamp ⇒ الوقت الي صار فيه log

لازم اظبط الاشيا بـ clock تبع R

(Config)# line Console 0

(Config-line)# login local

exit

(Config) # username Abeer pass 123

username Ahmed pass 456

login on-success log

لو صار login صح طلعلي log عالـ Server

login on-failure log

لو صار login غلط طلعلي log عالـ Server

Exit - Exit

username: abeer
password: 123

% sec-log-(5)-log
↳ Severity num.

Severity numbers:

- Emergency (severity 0)
- Alert (severity 1)
- Critical (severity 2)
- Error (severity 3)
- Warning (severity 4)
- Notification (severity 5)
- information (severity 6)
- debugging (severity 7)

(Config)# logging consol 6 ↵
معناه هيظهرلي Severity 6 فما تحت من sys log

(Config)# logging buffered 7
عبارة عن جزء من الـ Ram تابعة لـ R بالظبط عشان نخزن فيه الـ logs بتاعتي
logging buffered 5000
حجم الـ buffer ⇐ 5000 byte

R # debug IP packet ↵ يعمل debug على الـ IP

show logging ↵ علشان اشوف الـ log

clear logging ↵
↵ علشان اعمل clear للـ logs اللي في الـ buffer

(Config) # logging origin-id ?

عشان اللي جي يشتغل الـ log على السيرفر . بيتحط بالاسم الخاص بال R

(Config) # Logging origin-id hostname

(Config) # logging origin-id IP

اى log هيروح لل R هيظهر بال IP بتاع الرابط ده IP

(Config) # logging source-interface f0/0

اذا لم احدد ال source int هيظهر على ال syslog server ← 0.0.0.0

(Config) # logging origin-id string MY_ROUTER

logging trap 6 ابعت ال logs لل sys log server لحد severity 6

6 → by default

File -> Export setting from INI file

هفتح الملف واحدد مكانه ،
وافتح الملف اللي هو فيه ، عن طريق برنامج Kiwi viewer

Summary

logs Can be on :-
- Console
- terminals (R # terminal monitor)
- SNMP
- syslog servers
- buffer

syslog

R(Config)# security authentication failure rate 2 log

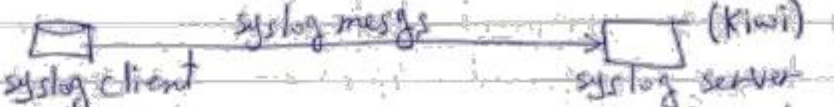
- هذا الأمر يحدد عدد مرات الـ auth مرتين قبل أن يعطي log للـ user بالخطأ الذي حدث أثناء الـ auth.

- الـ logs تظهر على الـ Console ولكن لا تخزن به ويمكن تخزين الـ logs في buffer.

R(Config) # logging buffered 5000

R# show logging

- كذلك يمكن تخزين الـ logs في syslog server.



- syslog [time stamp + log mesg name + severity level + text]

level	name	description
0	emergency	router unstable
1	alert	immediate action required
2	critical	condition critical
3	error	" error
4	warning	" warning
5	notification	normal but important event
6	info	info mesg
7	debugging	debug "

0 ← مثل عدم القدرة على تحميل الـ IOS ، 5 ← مثل عمل no shut على الـ int.

lab

① install Kiwi on the server

② R(Config) # logging on ← enable logging

③ # logging 192.168.1.2 ← Configure log host

④ # logging trap 0 ← (optional) def the severity level

⑤ # logging source-int f0 ← (optional) defines the src int

⑥ # logging origin-id اسم الراوتر ← (optional) define the router name or IP

- بعد تسطيب الـ Kiwi يظهر 2 short cuts على الـ desktop وهم Kiwi syslog daemon و Kiwi log viewer. والتي تظهر به رسائل الـ logs. وبجانب الساعة أيقونة الـ Kiwi يتحول لونها للأخضر إذا استلم البرنامج رسالة log،

- ونظهر log على الراوتر ثم الـ logs سوف تظهر على الـ Console ثم تختفي،

- في الـ viewer يظهر رقم الـ severity في جزء الـ msg بينما اسم الـ severity يظهر في الـ priority.

- في حالة وجود أكثر من راوتر في الشبكة ونريدها أن تظهر في الـ viewer بالاسم وليس بالـ IP نستخدم الأمر:

R(Config)# logging origin-id hostname ← يظهر باسم الراوتر

\# logging origin-id ip ← بالـ IP

\# logging origin-id string ← يظهر بـ ...

- اسم الراوتر أو الـ IP أو الـ text يظهر في الـ viewer في خانة الـ message.

- إذا استخدمنا أمر بحيث يظهر كـ IP فإنه يظهر 0.0.0.0 حتى يتم تحديد الـ source-int لأن الراوتر له أكثر من IP.

R(Config)# logging source-interface f0

- في برنامج الـ Kiwi يوجد icon شكل ▭▭ ندخل عليها ثم من severity tab تظهر احصائيات عن كل الـ logs بالـ severity الخاصة به.

- يمكن عمل save للـ logs ثم عرضها ببرنامج Kiwi-log viewer

file → export settings to ini file

ويتم عمل save للـ logs في ini file ثم فتحه بالـ notepad ويوجد داخله مسار تخزين الـ Cache file الذي به الـ logs.

C:\prog files\syslogd\logs\syslog catchall.text

وهذا الملف هو الذي يتم فتحه بالـ viewer

log viewer ⇒ file → open ← بالمسار

- لمسح الـ logs View → clear display

- R(Config)# logging on (enabled by default).

R # show log (to check if it's enabled)

syslog destinations [Console - monitor (Vty, AUX) - memory buffer - SNMP trap - flash]

R(Config) # logging 3 [means from 0 → 3]
R(Config) # logging Console debugging = logging Console 7
(disabled by default)

R(Config)# service sequence-numbers ← enables seq nu of the log
R(Config)# service timestamps ← enables time stamp of the log
service timestamps log ↵
<cr> datetime uptime ← time only not date since last reload

R# terminal monitor ← enable logging to telnet
- by default يتم ارسال severity6 الى ال syslogserver.
- او logging facility تسمى filters لل logs الى كل ال syslog ser
او تحديد شكل ال format لل logs.

R(Config)# no service timestamps log
no service timestamps debug
no service timestamps ← for log & debug

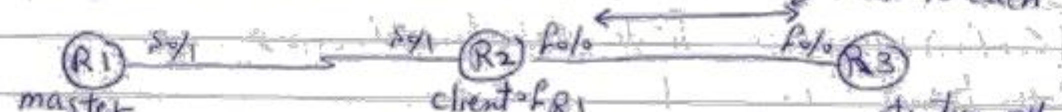
NTP (UDP 123)

- تقدم بأمر تكون السـاعة synchronized في الشبكة لمعرفة الوقت الصحيح لل syslogs، كذلك الـ digital certificates تعتمد على الـ time، وكذلك الـ authentication.

- في الـ hierarchy top الـ NTP يوجد الـ stratum-0 وهي عبارة عن atomic clock. ولكن لا يجوز لراوتر cisco يعمل time synch مع stratum-0 مباشرة.

- يمكن عمل سيرفر مثل جوجل عبر public NTP servers.

- NTP V3 is more secured than V1, V2. peer to each other



stratum no

R1(Config) # ntp master (or) ntp master 5

يمكن الاكتفاء بالأمر أو وضع رقم الـ stratum no.

- every next tree level has less accuracy.
- levels are known as stratum in NTP
- time always passed in UTC. (universal time Co-ordinated)
- NTP roles (server - client - peer)
  - server → supplies time but not adjust local
  - client → only adjusts to clock info
  - peer → synchronize each other. but must be in the same stratum.

- الـ edge router نجعله client لـ public NTP وداخل الشبكة نجعله peer لراوترات أخرى بحيث إذا فقد اتصاله بالـ public NTP فإنه يقوم بعمل synchronization مع أحد الـ peers.

- Key nu must match in NTP authentication.
- The client authenticates the server not the opposite because the server doesn't care who will get the clock.

lab R2(Config)#ntp server 10.0.0.1
ولكن يجب ملاحظة أن تكون ساعة R2 قريبة من R1 والا سيستغرق ساعات حتى يحدث synchronization.

R2# show ntp status
clock is synchronized, reference is 10.0.0.1
R2# debug ntp packet , debug ntp authentication
R2(Config)# ntp authenticate ← enable authentication
ntp authenticate-key 1 md5 CCIE
ntp trusted-key 1 (في حالة وجود أكثر من Key)
R2(Config)# ntp server 10.0.0.1 Key 1
R2# show ntp associations detail
Configured, authenticated
- by default فإنه يسمح في نقل الـ clock لأي client ولكن يمكن تحديد ذلك عن طريق ACL
R1(Config)# ntp access-group serve-only 1 (ACL nu)
R2(Config)# ntp source loop1
- كذلك يمكن ارسال الـ clock الى multicast group :
R1(Config-if)# ntp multicast 224.1.1.1
R2(Config-if)# ntp multicast client 224.1.1.1
- من debug ip packet نجد أن الـ NTP Port هو 123.
R2 # show clock detail
يظهر الوقت والـ time source حيث أخذناه من NTP.
R2 # show ntp associations
ماهو موجود هو * والتي تدل على أن الـ clock تكون synchronized ← *~ 10.0.0.1
R2 (Config)# ntp peer 11.0.0.3
R3(Config)# ntp peer 11.0.0.2

- اذا كان يوجد أكثر من ntp server يمكن تفضيل أحدهما بالأمر:

R(Config)# ntp server أ.ب.ج.د prefer

- اذا كان يوجد أكثر من key يمكن اختيار أحدهما:

R(Config)# ntp trusted-key 1

- يمكن تحديد أقصى عدد من الـ NTP servers التي يمكن عمل association معها:

R(Config)# ntp max-association ☐

- R(Config)# clock ?

summer-time   time-zone   hours offset from UTC

ex) R(Config)# clock time-zone EST 5

clock summer-time EST recurring مكرر

NetFlow (UDP)

- وظيفته مراقبة الشبكة والـ BW وتحليل الـ traffic وهو ليس حصري على سيسكو ويعمل على Juniper و H3C و Huawei و alcatel وغيرهم.
- ويقوم البروتوكول بجمع المعلومات وتخزينها في flow cache ليتم دفعها فيما بعد الى الـ Network analyzer، ويمكن أن يحدث لها timeout في الـ cache حيث يتم مسحها.
- والفرق بين الـ NetFlow والـ SNMP أن الأول يقوم بعمل push البيانات بينما الثاني يقوم بعمل pull البيانات.
- والفرق الثاني أن الـ SNMP يقوم بجمع معلومات أكثر عن الجهاز نفسه مثل الـ CPU والـ RAM utilization والـ traffic counts والـ resource errors، بينما الـ NetFlow يقوم بجمع معلومات مفصلة عن الـ traffic الذي يعبر الجهاز.
- ويعتمد الـ NetFlow على سبع طرق لجمع المعلومات وهي:

- Src IP add   - Dest IP add
- Src port for UDP or TCP   - Dest port for UDP or TCP
- IP add   - Ingress int   - IP ToS

- ويوجد versions للـ NetFlow و v5 هو أكثر استخداما وكذلك v9

ex1

Rz(Config)# int f0/0

Rz(Config-if)# ip route-cache flow

Rz(Config)# ip flow-export version 5 ← تحديد ال version

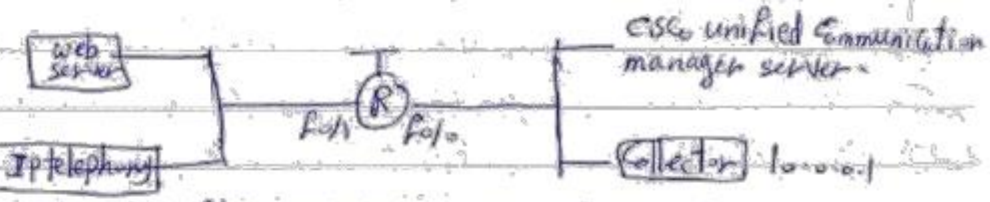
Rz(Config)# ip flow-export destination 10.0.0.1 2000

الأمر السابق لتحديد ال Ip ال Collector. وكذلك البورت الذي ستخدمه للإرسال لإرسال ال Netflow لأن يوجد له بورت معين.

Rz(Config)# ip flow-export source f0/0

الأمر لتحديد ال source الذي سيجمع منه المعلومات لإرسالها الى ال Collector.

ex2)



R (Config-if)# ip flow ingress ← f0/0 , f0/1

R (Config)# ip flow-export source loop 0

#ip flow-export version 5

#ip flow-export destination 10.0.0.1 5000

في المثال السابق سيقوم بمراقبة كلاً من f0/0 ، f0/1.

R(Config)# ip flow-cache timeout active 5

الأمر السابق لتحديد قيمة ال timeout الوقت الذي سيظل فيه المعلومات في الكاش قبل أن يحدث لها timeout.

R(Config)# ip flow-cache timeout inactive 30

R# show ip flow export

R# show ip cache flow

R# show ip cache verbose flow

- البرامج التي تستخدم كـ Collector مثل:-

- sflow Trend
- solarwind Netflow analyzer
- plixer scrutinizer
- Manage engine Netflow analyzer.

- ال Netflow يستخدم لعمل ال Collect لل info ال traffic الذي يخرج من ال int أو يدخل ال int.

Netflow

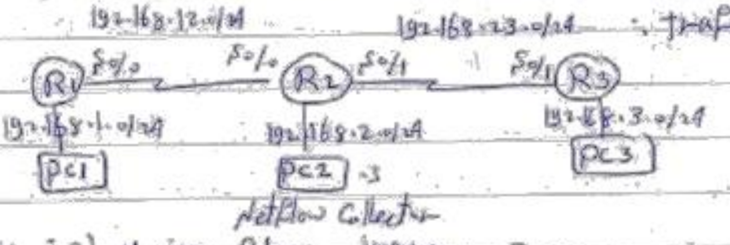
* monitors the traffic through the router

- عمل احصائيات عن الـ traffic اللي يمر عبر الراوتر والـ L3 sw ويقوم IP accounting

ويوجد flexible netflow وهو يستخدم netflow v9 ويمكن عمل customize

لـ traffic analysis:

lab



R2(Config-if)# ip flow ingress
ip flow egress } S0/0 & S0/1

R2(Config)# ip flow-export destination 192.168.2.3 9996

ال netflow [illegible] standard port [illegible]

R2(Config)# ip flow-export version [1 / 5 / 9]

R2# show ip flow interface

الأمر لمعرفة الـ ints اللي عامل عليها الـ netflow.

R2# show ip flow export

Destination(1) 192.168.2.3 (9996)

Version 9 flow records

نقوم بإنشاء traffic بين R1 و R3.

R1 # telnet R3 R3 # ping R1 repeat 1000

PC1 (browse to R3 ip http server)

R2 #show ip cache flow

R2 # clear ip flow stats

SNMP [L7 - UDP - port (161, 162)]

- بروتوكول لمراقبة الأجهزة والتحكم فيها عن بعد وكذلك عمل Config ،
- وهو تطوير لبروتوكول آخر اسمه SGMP (simple gateway mgmt protocol)
وجاء بعده بروتوكول آخر وهو CMIP (Secure Common mgmt info protocol)
ولكن لم يستمر طويلاً أمام الـ SNMP .

(R) ———————— [ ]

SNMP agent —— NMS (network mgmt station)

- SNMP mesgs [GET, GET-NEXT, GET-RESPONSE, SET, TRAP]

(R) ———————— [station]

① ← GET mesg 161

② GET-Response 161 →

③ ← GET-next 161 — متابعة المراقبة والحصول على المزيد من المعلومات

④ GET-Response 161 →

⑤ ← SET 161 — يطلب شيء ما تم تحديده نتيجة حدوث تغيير على الراوتر

⑥ TRAP 162 → — في حالة حدوث شيء ما للجهاز أو الـ station مثل توقف بورت عن العمل ويتم ارسالها على بورت 162 بينما باقي الرسائل على بورت 161 .

- وفي البداية يقوم الراوتر بوضع الـ info في MIB (mgmt information base) قبل ارسالها الى الـ mgmt station
- ويوجد 3 versions للـ SNMP : (V1, V2C, V3)
- في V2C تم استبدال Get-next بـ get-bulk والتي تستطيع حمل معلومات أكثر بالإضافة الى معلومات عن الـ security ، وبالنسبة لـ V3 تم اضافة authentication و privacy و access control . (V3 has authentication & encryption capabilities)

lab

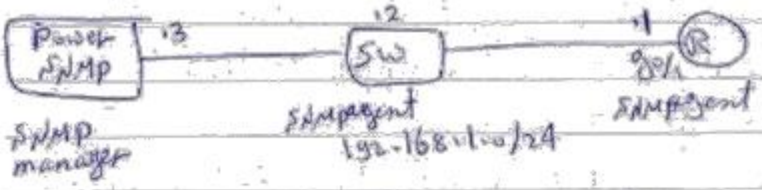
(R) f0/0 ———————— [station]

R(Config)# snmp-server Community CCIE ro / rw — recommended for security

SNMP lab

- نقوم بجلب الـ power SNMP free manager .

tools → Config → نعدل الـ IP الذي سيعمل عليه البرنامج



R(Config)# snmp-server Community CCIE ro SNMP_ACL (CCIE = pw, SNMP_ACL = named ACL)

\# snmp-server location snmp_manager } Comment

\# snmp-server contact abeer@cisco.com

\# snmp-server host 192.168.1.3 version 2c CCIE (key)

\# snmp-server enable traps ← enable all default traps

\# ip access-list standard SNMP_ACL

\# permit 192.168.1.3

- المفترض الآن أن يستلم البرنامج بعض الـ logs وإذا لم يحدث نقوم بعمل Copy run start وإذا لم يحدث نضغط SNMP agents ← Discover ونبحث في الـ IP 192.168.1.255 ومن خلال الأداة نضغط properties ونحدد الـ Community والـ version ، ومن البديهي المفترض أنه تم بالراوتر تحت v2 الـ SNMP ، ونقوم بنفس الأوامر على السويتش . ونقوم بعمل بعض الـ logs لإرسال الـ traps للبرنامج فتظهر في جزء الـ traps ، ثم نذهب لموقع سيسكو ونعمل search على SNMP object navigator ، ونختار MIBs download MIB SNMP obj navigator ونعمل كلك على SNMP obj navigator MIB locator page ، ثم نذهب لـ OIDs OID ونقوم بتحويل الـ OID .

SNMP (supported on almost all devices)

كل object له OID . objectID

ex)

R# show int fo/1

fo/1 (OID) is up (OID) , line protocol is up (OID)

MTU (OID) = — , delay (OID) = — , BW (OID) = —

ويقوم ال SNMP سيرفر بإرسال request للراوتر حتى يعرف حالة ال int

مثلا فيقوم الراوتر بإرسال حالة كل OID ، ويوجد داتابيز كاملة كترجمة ال OID اسمها MIB (mgmt information base) ، وهادة يتم بيعها مع الراوتر

* SNMP S/W [mRTG (open src) - PRTG - solarwins - Ciscoworks

* SNMP V2c → Community string clear text

* SNMP V3 → user based authentication - encryption - group

ووضع كل مجموعة من ال sensors في group ومعهم .

R(Config)# snmp-server community CISCO ro

نقوم بتطبيق ال PRTG وهو web-based application

Devices (tab) → R click on local device and add device → نكمل البيانات

ونختار automatic device identification

credentials for SNMP Device

(community) نكتب ال → Continue

وننتظر عليه حتى يقوم بعمل ال auto discovery